

Art Unit: 2431

DETAILED ACTION

This office is in response to remarks and amendments filed April 4, 2011. Claims 1, 6-9 and 11-20 are pending.

Drawings

The drawings submitted on August 14, 2008 are acceptable.

Response to Arguments

Applicant's arguments filed on April 4, 2011 have been fully considered. Applicant submitted amendments and previous rejection has been withdrawn.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Andrew T. Harry (56,959) on May 6, 2011.

IN THE CLAIMS

Please amend Claim 8 as follows:

8. (Currently Amended) An apparatus for performing cryptographic processing comprising:
- a cryptographic processor configured to encrypt data using pseudorandom sequences; and
 - a pseudorandom sequence generator configured to generate pseudorandom sequences, wherein the pseudorandom number generator is configured to include the apparatus comprising: ~~according to claim 1~~
 - a two-dimensional cellular automata random number generator configured to generate a first sequence;
 - a 2-by-L cellular automata random number generator configured to generate a second sequence;
 - a controllable cellular automata random number generator configured to generate a third sequence by determining cell states based on a corresponding cell control word and/or a corresponding rule control word, wherein the cell control word is generated by the 2-by-L cellular automata random number generator and the rule control word is generated by the two-dimensional cellular automata random number generator;
 - adders configured to perform bit-to-bit mod2 sum of the first, second and third sequences;

Art Unit: 2431

a first block configured to perform a nonlinear mapping on the summation results from the adders; and

a second block configured to perform a non-uniform decimation on the results of the nonlinear mapping, wherein the decimated result is outputted as a pseudorandom sequence.

Allowable Subject Matter

Claims 1, 6-9 and 11-20 are allowed over prior arts.

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in independent claims and subsequent dependent claims.

The following is an examiner's statement of reasons for allowance:

The present invention is directed to a method to produce pseudo random sequence, used in a cryptographic processor, by a pseudo random sequence generator that has adder which performs bit-to-bit combination of *two sequences produced with high and low randomness* from corresponding cellular automata,. The pseudo random sequence generator includes *two types of cellular automata* for generating the respective sequences with high and low randomness. An adder performs a bit-to-bit combination of the produced sequences from the corresponding cellular automata to output a pseudo random sequence and enables generating pseudo random sequences with maximum *controllable period* and statistical properties of randomness.

Thus, the cited prior art does not explicitly teach or suggest an apparatus for performing cryptographic processing comprising:

a cryptographic processor configured to encrypt data using pseudorandom sequences; and
a pseudorandom sequence generator configured to generate pseudorandom sequences,
wherein the pseudorandom number generator is configured to include the apparatus
comprising:

a two-dimensional cellular automata random number generator configured to generate a
first sequence;

Art Unit: 2431

a 2-by-L cellular automata random number generator configured to generate a second sequence;

a controllable cellular automata random number generator configured to generate a third sequence by determining cell states based on a corresponding cell control word and/or a corresponding rule control word, wherein the cell control word is generated by the 2-by-L cellular automata random number generator and the rule control word is generated by the two-dimensional cellular automata random number generator;

adders configured to perform bit-to-bit mod2 sum of the first, second and third sequences;

a first block configured to perform a nonlinear mapping on the summation results from the adders; and

a second block configured to perform a non-uniform decimation on the results of the nonlinear mapping, wherein the decimated result is outputted as a pseudorandom sequence.

1. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan J. Flynn can be reached on 571-272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SZ
May 8, 2011
/Syed Zia/
Primary Examiner, Art Unit 2431